AE

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CHARLES A. KRUMWIEDE,	)	
	)	
Plaintiff,	)	Case No. 05 C 3003
	)	
v.	)	Magistrate Judge
	)	Martin C. Ashman
BRIGHTON ASSOCIATES, L.L.C., and ISMAEL C. REYES,	)	
	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Defendant and Counterclaimant, Brighton Associates, L.L.C., moves this Court, pursuant to Rules 26 and 37 of the Federal Rules of Civil Procedure, to enter sanctions against Plaintiff and Counterdefendant, Charles A. Krumwiede, for spoliation of evidence. The parties have consented to have this Court conduct any and all proceedings in this case, including the entry of final judgment. *See* 28 U.S.C. § 636(c); Local R. 73.1(a).

After conducting an evidentiary hearing on March 16, 2006, the Court has carefully considered the testimony of witnesses who appeared at the hearing, the exhibits introduced into evidence, the written submissions of the parties and the arguments of counsel. The following are the Court's findings of fact and conclusions of law pursuant to Rule 52(a) of the Federal Rules of Civil Procedure. To the extent certain findings of fact may be deemed to be conclusions of law, they shall also be considered the Court's conclusions of law. Similarly, to the extent matters contained in the conclusions of law may be deemed findings of fact, they shall also be considered the Court's factual findings.

I. Findings of Fact

A. Parties

1. Brighton is a corporation licensed in the State of Illinois with its mailing address located at 117 South Cook Street, #165, Barrington, Illinois, and its principal place of business located at 10 Crawling Stone Drive, Barrington Hills, Illinois. (Compl. at 1-2.) Brighton is a consulting firm that provides document and project management solutions for clients in the life sciences, manufacturing, and services sectors.

2. Reyes is an individual who is the Chief Operations Officer, Technology, for Brighton and resides at 10 Crawling Stone Drive, Barrington Hills, Illinois. (Compl. at 2.)

3. Krumwiede is an individual who resides at 2118 Hollow Tree Court, Hebron, Kentucky. Krumwiede worked for Brighton as Director of Business Development from October 2002 until March 2005. (Compl. at 3-4.) Krumwiede left Brighton in 2005 and went to work as Director of Business Development for Strategic Technologies Inc. ("STI"), a competitor of Brighton.

B. Claims of the Parties

4. Krumwiede sued Brighton for breach of his Employee Agreement, reimbursement of back pay, intentional infliction of emotional distress, and reformation of the Employee Agreement. Brighton filed a counterclaim against Krumwiede alleging (1) breach of the non-compete provision of Krumwiede's Employee Agreement, (2) breach of the confidentiality provision of Krumwiede's Employee Agreement, (3) tortious interference with prospective economic advantage, (4) violation of the Illinois Trade Secrets Act, and (5) breach of duty.

(Am. Counter Cl. at 6-17.) The counterclaim includes Brighton's claim that Krumwiede went to work for a competitor, STI, and misappropriated a business opportunity with a prospective Brighton client, namely LifeScan Scotland, Ltd. (located in Inverness, Scotland). Brighton sought to recover the laptop computer that Krumwiede used when he worked for Brighton ("Brighton's laptop") in order to determine whether Brighton's data was used improperly after Krumwiede went to work for STI. Krumwiede did not give up possession of the computer immediately and Brighton alleges that Krumwiede used his extra time with the computer to destroy evidence relevant to Brighton's counterclaim. Brighton argues that severe sanctions should be imposed on Krumwiede for his misconduct.

5. Krumwiede counters that he did not intentionally destroy any evidence and that most of the allegedly destroyed evidence still exists on his personal laptop and probably on Brighton's laptop (with only insignificant alterations in the files' metadata) as well. Krumwiede also suggests that Brighton's counsel, Mr. Matthew F. Prewitt, compromised the neutrality of Forensicon, Inc., the third party that analyzed Brighton's laptop, by coaching Forensicon's employees and meddling in the creation of Forensicon's report. Finally, Krumwiede argues that LifeScan Scotland was not a business opportunity covered by his Employee Agreement so any files pertaining to LifeScan Scotland cannot constitute significant evidence and their destruction, alteration, or modification cannot justify severe sanctions.

C. Computer at Issue

6. Krumwiede purchased a laptop computer when he began working for Brighton. Several weeks later, Brighton reimbursed Krumwiede for the cost of the laptop computer. (Tr. at 177.)

7. While working for Brighton, Krumwiede used Brighton's laptop to coordinate sales calls for Brighton, prepare Brighton client proposals, and prepare Brighton pre-assessment reviews for clients or prospective clients. (Tr. at 159.)

8. Brighton terminated Krumwiede's employment in March 2005. (Compl. at 3-4.)

9. By agreement, Krumwiede was to return all Brighton property to Brighton after he was fired. (JX # 1.)[1] Krumwiede did return several items to Brighton but not Brighton's laptop. Mr. George Benevento, a former partner at Brighton, told Krumwiede that he did not need to return the computer. (Tr. at 192-93.) Mr. Benevento is not only Krumwiede's father-in-law but he left Brighton to work for STI at about the same time as Krumwiede and is currently engaged in litigation against Brighton. (Id.) Krumwiede was also under the impression that no Brighton employees were ever asked to return their computers after they had been dismissed, let go, or left the company. (Tr. at 178.)

10. On May 19, 2005, Krumwiede filed his lawsuit against Brighton. (Docket No. 1.)

11. On August 22, 2005, Krumwiede sent his own personal computer (not Brighton's laptop) to a service center to be fixed. (JX # 3.) That computer was shipped back to Krumwiede

[1] The joint exhibits submitted by the parties at the March 16, 2006 evidentiary hearing are cited as "JX." Exhibits that were submitted by Krumwiede alone are cited as "Pl.'s Ex."

on September 6, 2005, (JX # 5), and arrived at Krumwiede's residence on approximately September 9, 2005.

12. Krumwiede claims that, prior to sending his personal computer to a service center, he backed up the files on his personal computer by saving them on Brighton's laptop. (Tr. at 171.)

D. Notice to Krumwiede of Impending Litigation

13. On August 25, 2005, Brighton filed and served its Motion for Leave to File First Amended Counterclaim. (Docket Nos. 14-15.) At the same time that Brighton served a copy of it Motion for Leave on Krumwiede, Brighton's counsel also delivered to Krumwiede's counsel a letter demanding that Krumwiede return to Brighton the laptop computer that Brighton had furnished to Krumwiede for his use while employed by Brighton. (JX # 4.)

14. The August 25, 2005 letter reads:

> "[Brighton] demand[s] that Mr. Krumwiede immediately cease using the laptop computer and stop accessing any data on the laptop computer. [Brighton] further demand[s] that the laptop computer be returned immediately, without any alteration, modification, formatting, or deletion of any files, information, or other data contained on the laptop. Any changes to the contents of the computer will be regarded by Brighton as deliberate spoliation of evidence by Mr. Krumwiede."

(JX # 4, p. 2.)

15. Despite the August 25, 2005 letter, Krumwiede refused to return the laptop.

16. Krumwiede admits that he received the August 25, 2005 letter but decided not to comply with it because he believed that (1) the letter was an attempt by Brighton to harass him, (2) the laptop computer belonged to him and not Brighton, and (3) Brighton's claims against him

lacked merit. Additionally, Krumwiede claims that he needed to use the laptop computer until his personal computer was returned from the service center. (Tr. at 161, 185-86.)

17. On September 9, 2005, Brighton filed a Motion for Order Compelling Plaintiff Charles Krumwiede to Surrender Possession of Personal Computer. (Docket No. 19.) On September 15, 2005, the Court granted Brighton's motion and directed Krumwiede to surrender possession of the laptop computer by the close of business that same day. (Docket No. 23.) Krumwiede claims that he was not informed by the Court or his attorneys of the September 15, 2005 order until September 16, 2005. (Tr. at 167-68.) When Krumwiede failed to comply with the September 15, 2005 order, Brighton filed an Emergency Petition for Rule to Show Cause on September 16, 2005. (Docket No. 25.) At the hearing on the Emergency Petition, the parties agreed that Brighton's laptop computer would be placed in the custody of a neutral expert, Forensicon, Inc., who would perform a forensic analysis of the laptop hard drive. (Brighton's Mot. Sanctions, Ex. C, pp. 4-7.) Ultimately, Brighton's laptop computer was sent, via Federal Express, to Forensicon's Chicago, Illinois offices on September 16, 2005. (JX # 14, Exec. Summary, p. 1.)

E. Forensicon's Neutrality

18. Forensicon was retained jointly by the parties to serve as a neutral third party expert. (Pl.'s Ex. # 4.) Mr. Scott Jones, a senior forensic examiner at Forensicon, conducted the examination and prepared Forensicon's reports. (JX # 14, Ex. A.) Both counsel for Brighton and Krumwiede had the right to ask Jones questions and meet with him throughout his investigation, however, only Brighton's counsel, Prewitt, took advantage of that opportunity. (Tr. at 120.)

Jones met with Prewitt on three occasions before his March 6, 2006 deposition, at which time Prewitt offered to answer any procedural questions Jones might have. Prewitt also visited Forensicon's offices once prior to March 1, 2006, and Jones discussed his report with Prewitt. (Tr. at 117-118.) Prewitt asked Jones questions about the report but Jones did not make any changes to his report as a result of his contact with Prewitt. (Id.) Prewitt provided Jones with copies of the various pleadings in this case. (Tr. at 52.) Finally, Jones went to Prewitt's offices prior to the March 16, 2006 hearing. Jones never met with Krumwiede's counsel. (Tr. at 116-120.)

19. Prewitt's law firm, Greenberg Traurig LLP, has worked with Forensicon before. (Tr. at 134.)

20. Neither Prewitt's contact with Jones, nor Greenberg Traurig's other dealings with Forensicon, compromised the neutrality of Forensicon's investigation and report in this matter, as evidenced, in part, by the consistency of Forensicon's October 2005 report with its March 2006 report.

F. Forensicon's Findings

21. On September 27, 2005, Forensicon began investigating the data contained in Brighton's laptop. (JX # 14, Ex. B, p. 3.) Forensicon created a forensically valid copy of the laptop's hard drive using EnCase software. (Id.; Tr. at 45-47.) This was part of the imaging process that allowed Forensicon to examine the metadata and the content of the files on the computer without disturbing the laptop more than necessary. Metadata describes when a file was created, where it was stored, and what programs the computer uses to help access the file.

22. On October 5, 2005, Forensicon released a report to counsel for Brighton and Krumwiede detailing file activity and whether devices capable of transferring or storing file data were connected to the laptop. Jones did not meet with counsel for Brighton or Krumwiede prior to the release of the October 2005 report.

23. Forensicon's October 5, 2005 report focused on three significant sets of dates: August 25, 2005; August 26, 2005 through September 14, 2005; and September 15, 2005. According to the report, (a) 1,586 files were "Last Accessed" on August 25, 2005, and 1,486 additionally report an "Is Deleted" value of "Yes," (b) 14,074 files were "Last Accessed" in between August 26 and September 14, 2005, and 7,820 additionally report an "Is Deleted" value of "Yes," and (c) 13,317 files were "Last Accessed" on September 15, 2005, of which 8,988 files were created on or before April 14, 2005, and eight report an "Is Deleted" value of "Yes." (JX # 14, Ex. J, pp. 1-2.) "Is Deleted" does not necessarily mean that an entire file was deleted but rather that the original file entry was deleted. Thus, if a file is moved or read or deleted, the original file entry will be changed and it will report as "Is Deleted." (Tr. at 68-69, 144-45.) Any alteration of an original file entry may be significant, however, because the metadata contained in the entry changes, making it impossible to verify that the file is identical to the original, even if the file's content appears unchanged. (Id.) Jones explained that when a file entry reports as "Is Deleted," the "Last Accessed" date is often the best approximation for the time when the changes to the file occurred. (Id.)

24. The October 5, 2005 report also found twenty-one separate USBSTOR registry entries and numerous file entries that report being accessed in a batch process manner (whereby multiple files are accessed at the same time or in very close succession). According to Jones, the

USBSTOR registry entries and the batch process accessing of files suggest that external hardware and USB storage devices were connected to the laptop computer and that those devices provided opportunities to transfer files to other computers, storage devices, and/or media. The date and time file metadata for September 15, 2005, also supports files having been transferred from the laptop to another destination. Without examining other computers or devices which may have received such transferred data, however, Jones could not verify the success or extent of any such activities. (JX # 14, Ex. J, pp. 3-4.)

25. On March 1, 2006, Forensicon provided the parties with a more detailed report that incorporated the October 5, 2005 report and set out a detailed timeline of relevant events for Brighton's laptop. (JX # 14, Ex. B.) The March report timeline reads:

a. On August 22, 2005, Krumwiede shipped his personal laptop computer to California for repairs. (JX # 3.) This computer was packaged and shipped back to Krumwiede on September 6, 2005, (JX # 5), and Krumwiede received it a few days later.

b. On August 25, 2005, the day Brighton filed its counterclaim and sent the preservation letter to Krumwiede's attorney, over 1,580 files were "Last Accessed" and 1,486 additionally report an "Is Deleted" value of "Yes." (JX # 14, Ex. B, p. 1.)

c. From August 26, 2005 until September 14, 2005, 14,074 files were "Last Accessed" and 7,820 files additionally report an "Is Deleted" value of "Yes." (JX # 14, Ex. B, pp. 1-3.) Dates of significant activity include August 26, 2005 (approximately 2,208 deleted file entries report "Last Accessed"), August 28,

2005 (approximately 1,628 deleted file entries report "Last Accessed"), and September 12, 2005 (approximately 3,214 deleted file entries report "Last Accessed"). (Id.) On all but eight days during this twenty-day period, deleted file entries report "Last Accessed." (Id.)

d. August 28, 2005, September 6, 2005, September 7, 2005, September 8, 2005, and September 12, 2005, show USBSTOR registry entries and numerous file entries that report being accessed in a batch process manner, which support that external hardware and USB storage devices were connected to the laptop computer and that those devices provided opportunities to transfer files to other computers, storage devices, and/or media. (Id.)

e. On September 6, 2005, and September 12, 2005, file entries report that defragmentation utility was used on the laptop computer. (JX # 14, Ex. B, pp. 2-3.) Defragmentation utility programs pull file fragments together and are supposed to make computers function faster and more efficiently. (Tr. at 41-44, 74.) When file fragments are pulled together they may use unallocated space in the computer and, in the process, write over previously deleted files (which are often moved to the unallocated space on the computer). (Tr. at 74.) The result is that deleted files may no longer be recoverable.[2] According to Jones, he has been trained to look for use of defragmentation utility because it is a common tool used for covering up file transfers and deletions.

[2] While it may be technologically possible to recover some of this data, Jones testified that the cost could be in the millions of dollars. (Tr. at 41.)

f. On September 15, 2005, the day Plaintiff was ordered to surrender the laptop computer, Plaintiff used the laptop computer well past 7 p.m. (JX # 14, Ex. B, p. 3.) Plaintiff's activities on September 15, 2005, resulted in (1) eight deleted file entries reporting "Last Accessed," (2) multiple USBSTOR registry entries, and (3) over 13,000 file entries reporting "Last Accessed," including files named "SALES.ZIP" and "STI.ZIP." (Id.)

g. ZIP files function as archives capable of storing other file types with compression and can allow for concealment of data and easier transfer and storage of files.

h. Activity relating to the ZIP files named "SALES.ZIP" and "STI.ZIP" is particularly significant because these ZIP files displayed evidence of "nested" data, i.e., data that is concealed by storing it within multiple layers of other folders. (Tr. at 43-44.)

i. A large number of nested files is often evidence of a deliberate attempt to conceal information. Furthermore, metadata is often eliminated by the act of nesting files. (Tr. at 43.)

j. Forensicon's investigation revealed that "STI.ZIP" contains approximately eleven other zip files inside it, including one file whose contents display what clearly appears to be Brighton file data. (JX # 14, Ex. E.) Similarly, "SALES.ZIP" contains about 194 other ZIP files, some of which contain dates that are consistent with Krumwiede's employment with Brighton. (JX # 14, Ex. C.)

k. Entries for both "STI.ZIP" and "SALES.ZIP" also appear in "Lost Files." EnCase uses "Lost Files" to group file entries for which it can find no parent folder and cannot establish the original file path. Entries for both "STI.ZIP" and "SALES.ZIP" not only appear within "Lost Files," which suggests that ZIP files were moved from their original location, but the "STI.ZIP" and "SALES.ZIP" entries are both deleted and overwritten such that Forensicon could not determine their original file path. When the original file path cannot be determined, the metadata cannot be authenticated and one cannot know for certain whether any changes were made in the files. (JX # 14, Exec. Summary, p. 4.)

l. A search for all files containing the word "LifeScan" or "Inverness" revealed that 180 files containing the word "LifeScan" and seventy files containing the word "Inverness" were listed as "Is Deleted." (JX # 14, Exs. H-I.) As stated above, this does not mean that the "LifeScan" or "Inverness" files were necessarily deleted but it suggests that changes to the file metadata occurred.

m. Many files were deliberately erased from Brighton's laptop. Approximately 142 files were put in the laptop's recycle bin, of which 139 report being deleted. Of the 139 deleted files, 111 were both deleted and overwritten, such that only twenty-eight of these deleted files could possibly be recovered through the use of forensic tolls and techniques (none of these could be recovered using the Windows operating system itself). (JX # 15.) In order to delete and overwrite these 111 files, Krumwiede needed to deliberately select each file for

deletion, take steps to place those files in the recycle bin, and then take the additional step of purging the recycle bin. (Id.)

26. Based on his examination of activity that occurred between August 25, 2005 and September 16, 2005, Jones's expert opinion was that:

> The combination of a court order violation, deliberate movement of file data, admitted deletion activities, multiple use of defrag, use of ZIP file to conceal or transport Brighton Associates data, [and use of] multiple USB devices . . . [establishes that] Krumwiede did intend to destroy evidence and did intend to conceal the existence and/or movement of data in violation of defense's preservation letter dated August 25, 2005, as well as defy the Court's order dated 9/15/2005 to surrender the laptop.

(JX # 14, Exec. Summary, p. 5.)

27. Jones did not search the laptop's email, thoroughly explore the content of nested files, nor examine the laptop's archives, so he did not know the extent to which "deleted" or otherwise altered files were actually destroyed or lost. Rather, Jones's search was confined to those files described as "Lost Files" in the computer system (where the metadata of the files was not the exact original). (Tr. at 92-94.)

28. At the March 16, 2006 evidentiary hearing, Jones testified that the mere copying of data from one computer to another would not cause files on the original computer to register as "Is Deleted," and that a virus scanner would not affect the "Last Accessed" date of files listed as "Is Deleted." (Tr. at 137.)

G. Krumwiede Admits Using Brighton's Laptop After August 25, 2005.

29. Krumwiede admits that he performed defragmentation procedures on several occasions in September 2005. (Tr. at 186-88.) According to Krumwiede, as a computer

specialist, he performs defragmentation at least once a week as part of his normal routine. (Tr. at 187.) Krumwiede suggests that an examination of his personal laptop computer, now in STI's custody, would reveal that he performs defragmentation procedures on a regular basis. (Tr. at 189-90.)

30. Krumwiede admits that he used USB devices to transfer data off Brighton's laptop computer. Krumwiede claims that he temporarily stored confidential and proprietary STI information on the Brighton laptop computer so that he would have a back up copy of the files in case those files were lost or deleted when he sent his own personal computer to be repaired. (JX # 7, ¶¶ 10-14.) Krumwiede claims that he removed those files from the laptop computer before turning it over to Forensicon because they were not relevant to his work with Brighton and were the property of his new employer, STI. Krumwiede admits that he may have unintentionally altered or deleted Brighton files while performing these operations. (Tr. at 186.)

31. Krumwiede claims that no permanent destruction of files occurred because he has copies of all the files on his personal laptop. This claim has yet to be verified, as Krumwiede refused to produce his personal laptop for Brighton, sent his personal laptop to STI for safe keeping in December 2005, and refuses to ask STI to return the laptop or produce it for this lawsuit. Krumwiede claims that STI would fire him for violating the terms of his Nondisclosure/Confidentiality Agreement if he turned over his personal laptop to Brighton but admits that he never asked STI to return the laptop, never asked STI for permission to use its confidential information in this proceeding, and STI has never threatened to fire him. (Tr. at 168, 182-83.)

32. In fact, Krumwiede's Nondisclosure/Confidentiality Agreement explicitly exempts employees from the Agreement when an employee is required by law to turn over confidential information and reads:

> [Restrictions regarding nondisclosure of STI Confidential Information] shall not apply to any Confidential Information that . . . (b) is required by applicable law, legal process, or any order or mandate of a court or other governmental authority to be disclosed; or (c) is reasonably believed by Employee, based upon the advise of legal counsel, to be required to be disclosed in defense of a lawsuit or other legal or administrative action brought against Employees; provided that in the case of clauses (b) or (c), Employee shall give the Company reasonable advance written notice of the Confidential Information intended to be disclosed and the reasons and circumstances surrounding such disclosure, in order to permit the Company to seek a protective order or other appropriate request for confidential treatment of the applicable Confidential Information.

(JX # 2, p. 4.)

II. Conclusions of Law

A. Jurisdiction

1. This Court has jurisdiction over Brighton's cause of action pursuant to 28 U.S.C. § 1332.

2. Venue lies in the Northern District of Illinois pursuant to 28 U.S.C. § 1391(a) and § 1391(c).

B. Krumwiede's Actions Amount to Willful and Bad Faith Spoliation of Evidence and Warrant Default Judgment.

3. A party has a duty to preserve evidence, including any relevant evidence over which the party has control and reasonably knew or could reasonably foresee was material to a

potential legal action. *China Ocean Shipping (Group) Co. v. Simone Metals, Inc.*, No. 97 C 2694, 1999 WL 966447, at *2 (N.D. Ill. Oct. 1, 1999). *See also Boyd v. Travelers Ins. Co.*, 652 N.E.2d 267, 270 (Ill. 1995).

4. A formal discovery request is not necessary to trigger the duty to preserve evidence. *Danis v. USN Comm., Inc.*, No. 98 C 7482, 2000 WL 1694325, at *33 (N.D. Ill. Oct. 23, 2000). The filing of a complaint may alert a party that certain information is relevant and likely to be sought in discovery. *Cohn v. Taco Bell Corp.*, No. 92 C 5852, 1995 WL 519968, at *5 (N.D. Ill. Aug. 30, 1995).

5. The August 25, 2005 letter that Brighton sent to Krumwiede, as well as the August 25, 2005 notice of Brighton's counterclaim, alerted Krumwiede to the fact that the contents of the laptop would likely be relevant evidence in Brighton's legal action against him.

6. After receiving the August 25, 2005 letter and notice of Brighton's counterclaim, Krumwiede had a duty not to alter, destroy, or modify the contents of the laptop computer.

7. Once a party is on notice that files or documents in their possession are relevant to pending litigation, the failure to prevent the destruction of relevant documents crosses the line between negligence and bad faith, even where the documents are destroyed according to a routine document retention policy. *Wiginton v. CB Richard Ellis*, No. 02 C 6832, 2003 WL 22439865, at *7 (N.D. Ill. Oct. 23, 2003). Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of relevant documents. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). Spoliation of evidence occurs when one party destroys evidence relevant to an

issue in the case. *Smith v. United States*, 293 F.3d 984, 988 (7th Cir. 2002) (citing *Crabtree v. Nat'l Steel Corp.*, 261 F.3d 715, 721 (7th Cir. 2001)).

8. Krumwiede admittedly failed to put in place a litigation hold with respect to Brighton's laptop computer and continued to delete, alter, modify, and access thousands of files after being put on notice that the contents of the laptop computer were the subject of litigation. The deletion, alteration, and modification of these documents continued at least until 7 p.m. the night before Krumwiede turned Brighton's laptop computer over to Forensicon. (JX # 14, Ex. B, p. 3.)

9. This Court has discretion in imposing sanctions under Rule 37 or pursuant to its inherent power. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 44-45 (1991); *Quela v. Payco-Gen. Am. Creditas, Inc.*, No. 99 C 1904, 2000 WL 656681, at *7 (N.D. Ill. May 18, 2000). Sanctions for spoliation of evidence include awarding reasonable expenses, attorney fees, barring evidence or arguments, permitting adverse inferences, and dismissing claims. Fed. R. Civ. P. 37(b)(2)(A)-(D). *See also Crabtree*, 261 F.3d at 721. Where a party "fails to obey an order to provide or permit discovery," the court in which the action is pending may make such orders in regard to the failure as are just, including "[a]n order . . . dismissing the action or proceeding or any part thereof, or rendering a judgment by default against the disobedient party." Fed. R. Civ. P. 37(b)(2)(C). Any sanctions must, however, be proportionate to the circumstances surrounding the failure to comply with discovery. *Quela*, 2000 WL 656681, at *8 (internal quotations omitted).

10. Brighton seeks a default judgment. A default judgment is a harsh sanction that should only be employed in extreme situations where there is clear and convincing evidence of

willfulness, bad faith or fault by the noncomplying party. *Maynard v. Nygren*, 332 F.3d 462, 468 (7th Cir. 2003); *Wiginton*, 2003 WL 22439865, at *6. Willfulness, like bad faith, is associated with conduct that is intentional or reckless. *Long v. Steepro*, 213 F.3d 983, 987 (7th Cir. 2000). Fault does not refer to the noncomplying party's subjective motivation, but rather describes the reasonableness of the conduct. *Langley v. Union Elec. Co.*, 107 F.3d 510, 514 (7th Cir. 1997). Fault may be evidenced by negligent actions or a flagrant disregard of the duty to preserve potentially relevant evidence. *Diersen v. Walker*, No. 00 C 2437, 2003 WL 21317276, at *5 (N.D. Ill. June 6, 2003).

11. Clear and convincing evidence establishes that Krumwiede acted willfully and in bad faith when he continued to alter, modify, and destroy evidence after August 25, 2005. Beginning on August 25, 2005, Krumwiede had a duty not to alter, destroy, or modify the contents of Brighton's laptop computer. Despite this duty to preserve evidence, Brighton's laptop experienced a spike in activity between August 25, 2005 and September 16, 2005, that resulted in the alteration, modification, or destruction of thousands of potentially relevant files and their metadata. Particularly troubling is the tremendous increase in activity immediately following Krumwiede's receipt of the August 25, 2005 letter (especially from August 25 to August 28, 2005) and the September 15, 2005 order. In fact, it appears that Krumwiede worked late on September 15, 2005, in order to complete as many file transfers, alterations, and modifications as possible before relinquishing control of the laptop computer on September 16, 2005, and that Krumwiede lied to this Court when he testified that he did not receive notice of the September 15, 2005 order until September 16, 2005.

12. While the volume and timing of Krumwiede's activities are sufficient to find willful and bad faith spoliation of evidence, it is also clear that Krumwiede specifically altered and deleted potentially adverse evidence directly relevant to Brighton's claims. Of the altered or deleted files in this case, over 200 different files contained the words "LifeScan" or "Inverness." (JX # 12, Exs. H-I.) Without even delving into the merits of Brighton's claims, these 200 files appear to relate directly to Brighton's claims for breach of non-compete provision, breach of confidentiality provision, tortious interference with prospective economic advantage, and violation of the Illinois Trade Secrets Act.

13. Krumwiede's willfulness and bad faith are further evidenced by his continued obstruction of discovery even after relinquishing control of Brighton's laptop computer. In his December 9, 2005 response to Brighton's motion for sanctions, Krumwiede denied allegations of intentional spoliation of evidence, claiming instead that he stored confidential STI information on Brighton's laptop when his own computer was being repaired and then removed those files from Brighton's laptop before turning it over to Forensicon in order to avoid breaching his Nondisclosure/Confidentiality Agreement with STI. (Pl.'s Resp. Def.'s Mot. for Sanctions at 1-3.) Krumwiede claimed—and continues to claim—that no evidence was intentionally destroyed and that all the files in question either exist on Brighton's laptop or on his own personal laptop. However, immediately after filing his December 9, 2005 response, and before his claims could be verified or his personal laptop analyzed, Krumwiede shipped his personal computer to STI for safe keeping, again arguing that his Nondisclosure/Confidentiality Agreement with STI prevented him from turning over the computer. (Tr. at 181-83.) To date,

Krumwiede refuses to ask STI to return his laptop because he has a feeling STI will fire him if he makes the request.[3]

As noted above, Krumwiede's Nondisclosure/Confidentiality Agreement with STI does not apply when STI employees are required by law to produce evidence. Furthermore, despite Krumwiede's hunch, there is no evidence to suggest that STI will fire Krumwiede if he asks for his personal laptop. On the other hand, there is evidence—provided by this Court to Krumwiede—that a default judgment may be entered against Krumwiede if he fails to produce his laptop computer and substantiate his defenses to the spoliation of evidence claims. Nevertheless, Krumwiede refuses to ask for his personal laptop. Based on these facts, the Court finds Krumwiede's actions with regard to his personal laptop computer to be an egregious attempt to "hide the ball" and a flagrant discovery violation.

14. A party suffers prejudice due to spoliation of evidence when the lost evidence prevents the aggrieved party from using evidence essential to its underlying claim. *Langley*, 107 F.3d at 515; *In re Old Banc One S'holders Sec. Litig.*, No. 2005 C 2100, 2005 WL 3372783, at *4 (N.D. Ill. Dec. 8, 2005). Brighton was relying on the evidence contained in its laptop computer to establish that Krumwiede used Brighton's secrets and confidential information improperly and interfered with Brighton's business and clients. As a result of Krumwiede's spoliation of evidence, even if the thousands of altered and modified documents located on Brighton's laptop are not actually deleted, the changes to the file metadata call the authenticity of the files and their content into question and make it impossible for Brighton to rely on them.

---

[3] Brighton is now attempting to gain access to Krumwiede's laptop computer in a separate action against STI in Pennsylvania.

Furthermore, at least 111 files were deliberately deleted and overwritten and are no longer recoverable. It follows that, as a result of Krumwiede's actions, Brighton may no longer rely on evidence essential to its underlying claims and Brighton has been prejudiced by Krumwiede's spoliation of evidence.

15. Default judgment as to Brighton's claims for (1) breach of non-compete provision of Krumwiede's Employee Agreement, (2) breach of confidentiality provision of Krumwiede's Employee Agreement, (3) tortious interference with prospective economic advantage, and (4) violation of the Illinois Trade Secrets Act is the only appropriate remedy. In deciding between default and lesser sanctions, the Court considers (1) prejudice to Brighton, (2) prejudice to the judicial system, and (3) deterrence and punishment. *Quela*, 2000 WL 656681, at *8. In this case, Krumwiede's conduct shows such blatant contempt for this Court and a fundamental disregard for the judicial process that his behavior can only be adequately sanctioned with a default judgment. *See, e.g., QZO, Inc. v. Moyer*, 594 S.E.2d 541 (S.C. Ct. App. 2004) (upholding default judgment where appellant violated temporary restraining order by failing to comply with the order for seven days and reformatting hard-drive before producing the computer at issue). Entering a default judgment against Krumwiede will send a strong message to other litigants, who scheme to abuse the discovery process and lie to the Court, that this behavior will not be tolerated and will be severely sanctioned. *Quela*, 2000 WL 656681, at *8. Furthermore, any sanction less than default on these counts will not cure the prejudice already suffered by Brighton.

16. In addition to default judgment, Brighton is entitled to an award of costs and fees relating to its motion for sanctions, including Forensicon's fees and Brighton's reasonable attorneys' fees. *See* Fed. R. Civ. P. 37(b)(2), 37(c)(1). These expenses were incurred as a direct result of Krumwiede's misconduct and he shall bear those costs. Brighton is given leave to file a petition detailing these fees and costs within thirty days.

17. Finally, all data stored on Brighton's laptop shall be disclosed immediately to Brighton's attorneys, for attorneys' eyes only. In the event that any files on the computer appear to be STI's confidential information, Brighton's attorneys will withhold those files from Brighton, inform STI, and inform this Court and an appropriate protective order will be entered. All nonconfidential information shall be disclosed to Brighton immediately.

III. Conclusion

For the reasons stated above, the Court enters default judgment in favor of Brighton on Counts I, II, III, and IV of its counterclaim against Krumwiede for (1) breach of the non-compete provision of Krumwiede's Employee Agreement, (2) breach of the confidentiality provision of Krumwiede's Employee Agreement, (3) tortious interference with prospective economic advantage, and (4) violation of the Illinois Trade Secrets Act. Furthermore, Brighton is awarded its reasonable costs and fees, including attorneys' fees and the fees billed to Brighton by Forensicon. Finally, all data stored on Brighton's laptop shall be disclosed to Brighton's attorneys and ultimately, except as set out in paragraph 17 above, to Brighton. Trial will be held

on the issue of damages as to the claims on which default judgment has been entered herein on a date to be set by the Court. This matter is set for status on June 19, 2006.

MARTIN C. ASHMAN
United States Magistrate Judge

Dated: May 8, 2006.

Copies have been mailed to:

SCOTT P. ZOPPOTH, Esq.
BRYAN M. CASSIS, Esq.
Scott P. Zoppoth, PLLC
1800 Kentucky Home Life Building
239 South Fifth Street
Louisville, KY 40202

RONALD A. ORNER, Esq.
Ronald A. Orner & Associates
200 North LaSalle Street
Suite 1920
Chicago, IL 60601

Attorneys for Plaintiff

GREGORY E. OSTFELD, Esq.
MATTHEW F. PREWITT, Esq.
Greenberg Traurig, LLP
77 West Wacker Drive
Suite 2500
Chicago, IL 60601

Attorneys for Defendants